5 November 2021

CPA Australia Ltd
ABN 64 008 392 452

Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677
Website cpaaustralia.com.au

Digital Transformation Agency
PO Box 457
Canberra City
ACT 2601

By email: digitalidentity@dta.gov.au

Dear Sir / Madam,

Submission on the Australian Government's Digital Identity Legislation – Phase 3

CPA Australia represents the diverse interests of more than 168,000 members working in 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

CPA Australia supports policy initiatives that underpin the government's Digital Economy Strategy. However, such policies need to be balanced by appropriate standards of data privacy and security, and investment in suitable technologies to support both. While we believe that the national Trusted Digital Identity System (TDIS) is a major milestone and will facilitate the expansion of Australia's digital economy, we have the following concerns:

Data stewardship and data security

We have concerns about data profiling, identity theft and other risks to individuals' privacy if no or insufficient access controls and/or other safeguards are implemented that prevent accredited entities from being able to, for instance, connect different data points and single identifier attributes.

To overcome such risks, we recommend the government considers approaches taken by other jurisdictions. For example, in the course of developing the "iAM Smart" platform the Hong Kong Office of the Government Chief Information Officer (OGCIO) announced the adoption of access control and a monitoring mechanism for OGCIO staff who need to access personal data.

With regard to its system management, the OGCIO states that it will ensure that the core data (including users' personal data) in the "iAM Smart" system are encrypted using the prevailing internationally recognised Advanced Encryption Standard. To enhance data security, the data will be stored onshore in government data centres. Additionally, to conform with industry encryption standards, Transport Layer Security will also be adopted to encrypt data to ensure data security and integrity during transmission over the internet. The OGCIO will also manage and protect user data and privacy in accordance with international standards ISO 27001 and ISO 27701.

Holding, storing, handling or transferring digital identity information outside Australia

The Exposure Draft (ED) states that TDI rules may prohibit entities onboarded to the TDIS from holding, storing, handling or transferring digital identity information outside of Australia unless an exemption is granted. The use of common data storage solutions such as cloud technology, of which many providers offer offshore storage solutions, may pose practical challenges with respect to where data is held. It may prevent some entities from being eligible to onboard on to the TDIS. We note that The Privacy Act does not prevent a regulated entity from engaging a cloud service provider to store or process personal data offshore. The regulated entity must however comply with the

Australian Privacy Principles in sending personal data to the offshore cloud service provider, just as they need to for any other overseas outsourcing arrangement.

Retention and disposal of digital identity information

We notice that the ED neither states safeguards relating to the retention of digital identity information, nor elaborates on the disposal of such information. Further, relevant sections are not directly linked to Australian Privacy Principles.

As emphasised in our previous submission on the Digital Identity Legislation Position Paper, we suggest the government clarifies data deletion policies.

Accreditation

As the TDIF Rules do not mention for how long the TDIF accreditation is valid, we assume that the accreditation is valid indefinitely. This poses the question of whether the entity, once accredited, is required to undergo any review or audit to demonstrate that it continues to meet accreditation criteria. Given their handling of sensitive digital identity information, we recommend accredited entities should undergo frequent reassessments and "health checks". This is a significant matter given the importance of data security and, in this regard, the use of up-to-date technology.

Inclusion

We are concerned about the potential exclusion of those who do not own the required hardware (smart phones and other devices) and/or do not have internet access. The Digital Identity is not only the cornerstone of Australia's Digital Economy but also the access point to request and make use of public services. Australians who are not sufficiently technology-savvy, live in remote areas and/or are vulnerable, are at risk of being unable to partake in the digital economy and prevented from benefitting from the opportunities the digital economy offers. It is our view that the government should consider how to include those groups through education, investment in technological infrastructure and subsidies.

Definition of relying party

We understand that the definition of "relying party" is not intended to include tax agents assisting their individual clients prepare tax returns. This, however, is not clear in the exposure draft legislation or the supporting material.

We therefore recommend that the explanatory material to the legislation includes specific common examples of what would be a 'relying party' and what would not. In addition, the explanatory material could also include a discussion on whether a financial planner providing advice to a client is a relying party and whether business to business transactions could be covered by the regime.

If you have any questions about this submission, please do not hesitate to contact Dr. Jana Schmitz, Technical Advisor, Assurance and Digital Economy Policy at CPA Australia on jana.schmitz@cpaaustralia.com.au.

Yours sincerely

Dr Gary Pflugrath FCPA
Executive General Manager, Policy and Advocacy